

Notice of Allowability

Application No.

10/016,392

Examiner

Tamara Teslovich

Applicant(s)

BATCHER, KENNETH W.

Art Unit

2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to Application filed on 10 December 2001.
2. ☒ The allowed claim(s) is/are 1-20 and 22-27.
3. ☒ The drawings filed on 2 February 2002 are accepted by the Examiner.
4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) ☐ All b) ☐ Some* c) ☐ None of the:
 1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
 6. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
 - (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
 - 1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
 - (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.
- Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
7. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3. ☒ Information Disclosure Statements (PTO-1449 or PTO/SB/08),
Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit
of Biological Material

5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☐ Interview Summary (PTO-413),
Paper No./Mail Date _____
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____



ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER

DETAILED ACTION

ELECTION / RESTRICTION

Restriction to one of the following inventions is required under 35 U.S.C. 121:

- I. Claims 1-28, drawn to a system/method for encrypting/decrypting data, classified in class 380, subclass 42.
- II. Claims 29-35, drawn to a bit table used to track memory, classified in class 711, subclass 205.

Inventions I and II are related as combination and subcombination. Inventions in this relationship are distinct if it can be shown that (1) the combination as claimed does not require the particulars of the subcombination as claimed for patentability, and (2) that the subcombination has utility by itself or in other combinations (MPEP § 806.05(c)). In the instant case, the combination as claimed does not require the particulars of the subcombination as claimed because the various components in the combination share functions allocated supremely to the bit table in the subcombination. The subcombination has separate utility such as recording changes made to a memory to be undone within a restore function for a computer system.

Because these inventions are distinct for the reasons given above and have acquired a separate status in the art as shown by their different classification, restriction for examination purposes as indicated is proper.

During a telephone conversation with Attorneys John X. Garred and Larry Donovan on May 25, 2005 a provisional election was made without traverse to

Art Unit: 2137

prosecute the invention of I, claims 1-28. In a subsequent interview on May 31, 2005, Larry Donovan agreed to an examiner's amendment canceling the claims directed to the nonelected invention.

EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it **MUST** be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Larry Donovan on 31 May 2005.

The application has been amended as follows:

Please amend Claims in accordance with Examiner's "Amendment to the Claims" included as pages 4-7 of this office action.

Please amend Specification in accordance with Examiner's "Amendment to the Specification" included as page 8 of this office action.

AMENDMENT TO THE CLAIMS

1. (Currently Amended) A system for encrypting data, comprising:
 - a memory for storing ~~permutating~~ permuting data values for ~~decryption~~ encryption;
 - a bit table for tracking data modifications within the memory; and
 - a controller for executing an encryption algorithm wherein a plurality of data values are read concurrently from the memory ~~generally simultaneously~~ to determine a plurality of index values, and a plurality of pairs of data values stored in the memory are respectively swapped concurrently within the memory ~~generally simultaneously~~, said plurality of pairs of data values identified by said plurality of index values.
2. (Original) The system of claim 1 wherein the memory is a dual port RAM memory for allowing simultaneous read and write operations.
3. (Original) The system of claim 1 wherein the memory is a single port RAM memory.
4. (Original) The system of claim 1 wherein said controller includes an implementation for detecting when said plurality of pairs of data values have been modified.
5. (Original) The system of claim 1 wherein the bit table comprises one bit per location in the memory.
6. (Original) The system of claim 1 further comprising a key memory for storing in consecutive order a plurality of keys respectively associated with a plurality of data frames including encrypted data, wherein each said key is comprised of a plurality of key values.

Art Unit: 2137

7. (Original) The system of claim 6 wherein the key memory comprises a dual port RAM memory.

8. (Currently Amended) A system for decrypting data, comprising:

a memory for storing ~~permutating~~ permuting data values for decryption;

a bit table for tracking data modifications within the memory; and

a controller for executing an ~~encryption~~ decryption algorithm wherein a plurality of data values are read concurrently from the memory ~~generally simultaneously~~ to determine a plurality of index values, and a plurality of pairs of data values stored in the memory are respectively swapped concurrently within the memory ~~generally simultaneously~~, said plurality of pairs of data values identified by said plurality of index values.

9. (Original) The system of claim 8 wherein the memory is a dual port RAM memory for allowing simultaneous read and write operations.

10. (Original) The system of claim 8 wherein the memory is a single port RAM memory.

11. (Original) The system of claim 8 wherein said controller includes an implementation for detecting when said plurality of pairs of data values have been modified.

12. (Original) The system of claim 8 wherein the bit table comprises one bit per location in the memory.

13. (Original) The system of claim 8 further comprising a key memory for storing in consecutive order a plurality of keys respectively associated with a plurality of data frames including encrypted data, wherein each said key is comprised of a plurality of key values.

Art Unit: 2137

14. (Original) The system of claim 13 wherein the key memory comprises a dual port RAM memory.

15. (Currently Amended) A method for encrypting data, comprising:

storing ~~permutated~~ permuted data values for encryption;

tracking data modifications during the step of storing ~~permutating~~ permuting values; and

executing an encryption algorithm wherein a plurality of data values are read concurrently from the stored ~~permutating~~ permuting data values ~~generally simultaneously~~ to determine a plurality of index values, storing a plurality of pairs of data values, and respectively swapping concurrently ~~generally simultaneously~~, said plurality of pairs of data values identified by said plurality of index values.

16. (Original) The method of claim 15 comprising a step of detecting when said plurality of pairs of data values have been modified.

17. (Currently Amended) The method of claim 15 comprising a step of forwarding the stored ~~permutating~~ permuting data values when said data values have common data storage locations to correctly compute an out of order sequence of data manipulation during a same clock cycle.

18. (Original) The method of claim 15 wherein read/write operations between different algorithm iterations are mapped to different ports on a data memory in the same clock cycle.

19. (Currently Amended) The method of claim 15 ~~of~~ comprising a step of examining the stored data values to see if a simultaneous read/write operation is required.

20. (Original) The method of claim 15 further comprising the step of storing in consecutive order a plurality of keys respectively associated with a plurality of data

frames including encrypted data, wherein each said key is comprised of a plurality of key values.

21. (Canceled)

22. (Currently Amended) A method for decrypting data, comprising:

storing ~~permutated~~ permuted data values for decryption;
tracking data modifications during the step of storing ~~permutating~~ permuting values; and
executing an encryption algorithm wherein a plurality of data values are read concurrently from the stored ~~permutating~~ permuting data values ~~generally simultaneously~~ to determine a plurality of index values, storing a plurality of pairs of data values, and respectively swapping concurrently ~~generally simultaneously~~, said plurality of pairs of data values identified by said plurality of index values.

23. (Original) The method of claim 22 comprising a step of detecting when said plurality of pairs of data values have been modified.

24. (Currently Amended) The method of claim 22 comprising a step of forwarding the stored ~~permutating~~ permuting data values when said data values have common data storage locations to correctly compute an out of order sequence of data manipulation during a same clock cycle.

25. (Original) The method of claim 22 wherein read/write operations between different algorithm iterations are mapped to different ports on a data memory in the same clock cycle.

26. (Currently Amended) The method of claim 22 ~~of~~ comprising a step of examining the stored data values to see if a simultaneous read/write operation is required.

Art Unit: 2137

27. (Original) The method of claim 22 further comprising the step of storing in consecutive order a plurality of keys respectively associated with a plurality of data frames including encrypted data, wherein each said key is comprised of a plurality of key values.

28. (Canceled)

29-35. (Canceled)

AMENDMENT TO THE SPECIFICATION

Please replace the paragraph beginning on page 6, line 16 with the following rewritten paragraph:

According to the present invention there is provided a system for expedited encryption and decryption operations including a first dual port memory for storing in consecutive order a plurality of keys respectively associated with a plurality of data frames including encrypted data, wherein each said key is comprised of a plurality of key values; a second dual port memory for storing ~~permutating~~permuting data values for decryption; a bit table for tracking data modifications within the second dual port memory; and a controller for executing a decryption algorithm wherein a plurality of data values are read concurrently from the second dual port memory ~~generally simultaneously~~ to determine a plurality of index values, and a plurality of pairs of data values stored in the second dual port memory are respectively swapped concurrently within the second dual port memory ~~generally simultaneously~~, said plurality of pairs of data values identified by said plurality of index values. The controller contains a means of controlling the data path and dual ported memory so that conflicts between simultaneous overlapping operations are resolved.

REASONS FOR ALLOWANCE

The following is an examiner's statement of reasons for allowance:

The present invention is directed to a hardware-based data encryption/decryption system employing a dual ported memory table and method for fast table initialization. Each independent claim identifies the uniquely distinct feature of a "bit table for tracking data modifications within the memory" wherein 'data modifications' comprise reading a plurality of data values concurrently from the memory to determine a plurality of index values to facilitate the swapping within memory of the plurality of pairs of data values identified by said plurality of index values. The closest prior art, Matthews, Jr. (U.S. 6,549,622 B1) utilizes multi-port RAM memory to cut the necessary clock cycles in half but fails to disclose the use of a bit-table to track data modifications within the memory. Rose and Hawkes' *"Turing: A Fast Stream Cipher"*, Kitsos et al.'s *"Hardware Implementation of the RC4 Stream Cipher"*, Galanis et al.'s *"Comparison of the Performance of Stream Ciphers for Wireless Communications"* and Hamalainen et al.'s *"Hardware Implementation of the Improved WEP and RC4 Encryption Algorithms for Wireless Terminals"* are also considered relevant to the present invention but fail to disclose a "bit table for tracking data modifications within the memory" within their encryption and decryption systems. The prior art, either singularly or in combination, fail to anticipate or render the above underlined limitations obvious.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably

Art Unit: 2137

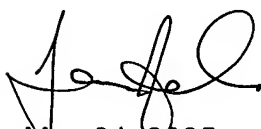
accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

CONCLUSION

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tamara Teslovich whose telephone number is (571) 272-4241. The examiner can normally be reached on Mon-Fri 8-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).


May 31, 2005
T. Teslovich


ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER